This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

FIG. 1

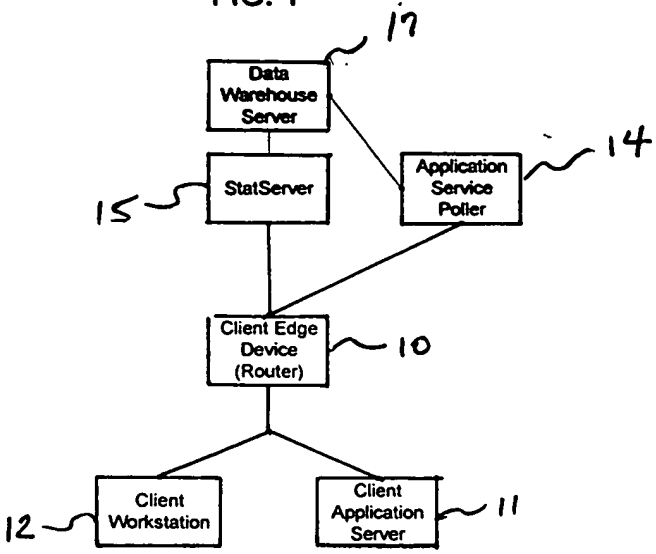
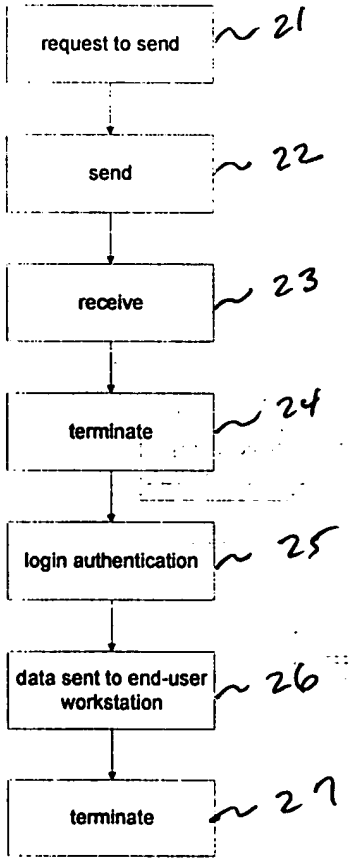

Data Warehouse Server
17
StatServer
15
Application Service Poller
14
Client Edge Device (Router)
10
Client Workstation
12
Client Application Server
11

FIG. 2


request to send
21
send
22
receive
23
terminate
24
login authentication
25
data sent to end-user workstation
26
terminate
27

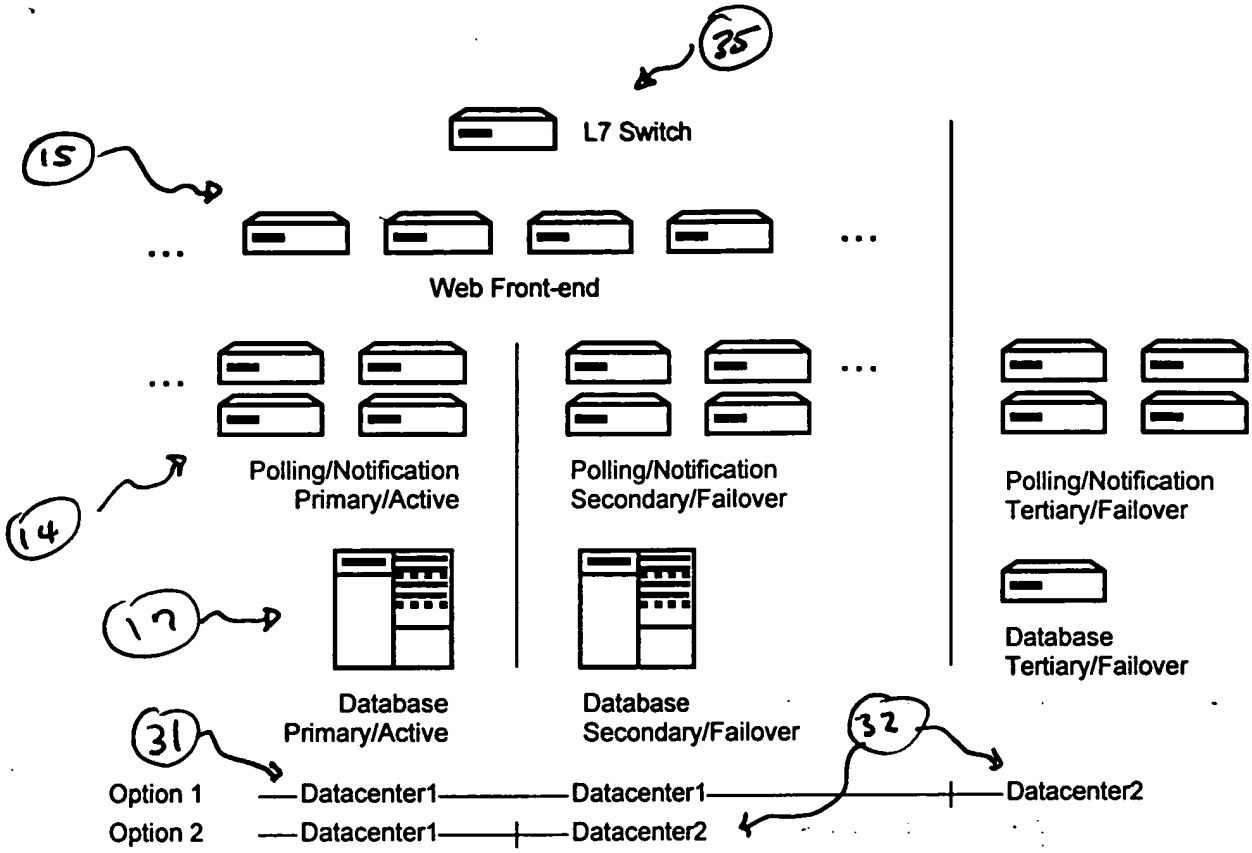

35
L7 Switch
15
Web Front-end
Polling/Notification
Primary/Active
Polling/Notification
Secondary/Failover
Polling/Notification
Tertiary/Failover
14
17
Database
Primary/Active
Database
Secondary/Failover
Database
Tertiary/Failover
31
32
Option 1
Datacenter1
Datacenter1
Datacenter2
Option 2
Datacenter1
Datacenter2

FIG. 3

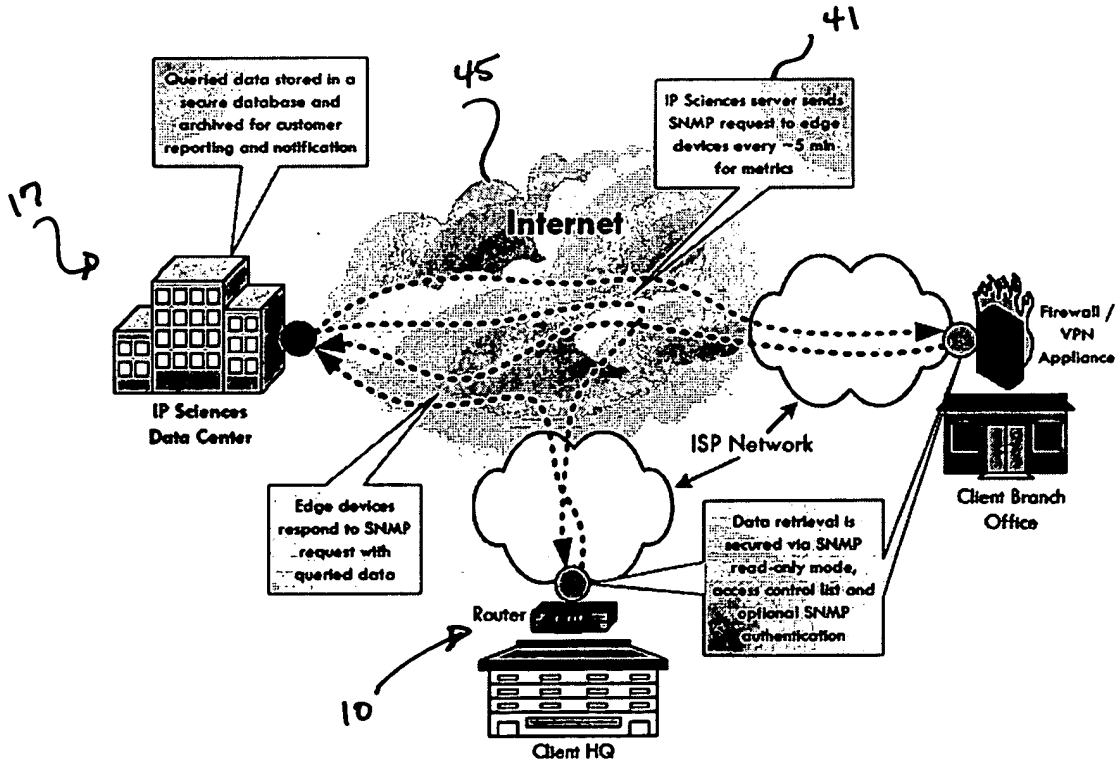
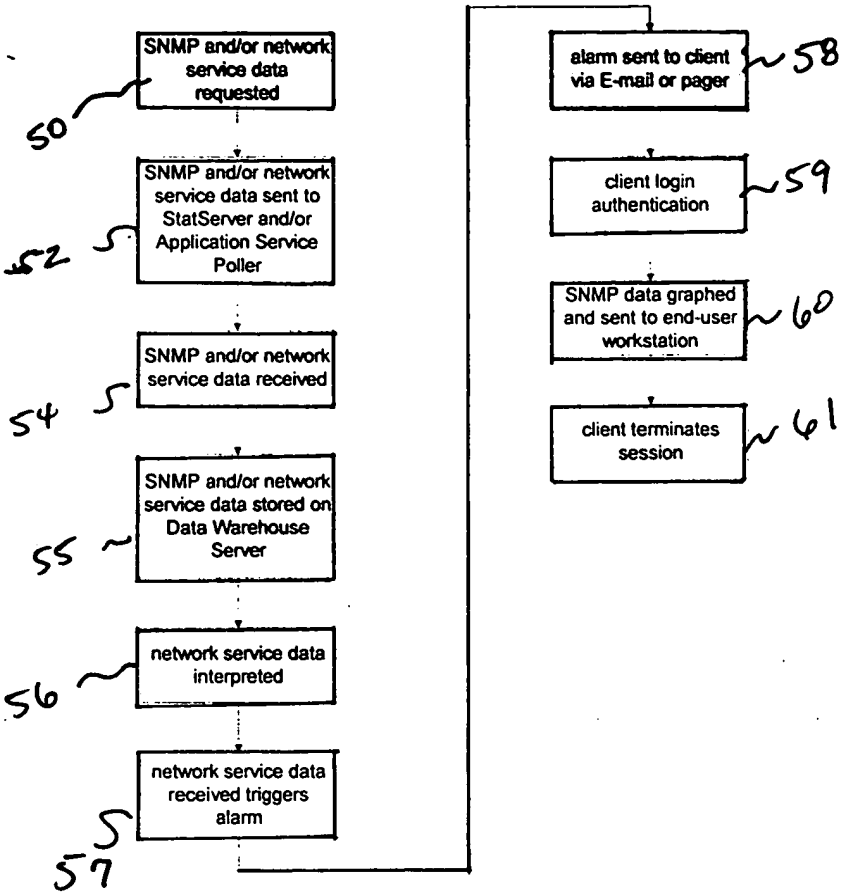

41
45
Queried data stored in a secure database and archived for customer reporting and notification
IP Sciences server sends SNMP request to edge devices every ~5 min for metrics
17
Internet
Firewall / VPN Appliance
IP Sciences Data Center
ISP Network
Client Branch Office
Edge devices respond to SNMP request with queried data
Data retrieval is secured via SNMP read-only mode, access control list and optional SNMP authentication
Router
10
Client HQ

FIG. 4

FIG. 5


SNMP and/or network service data requested
50
SNMP and/or network service data sent to StatServer and/or Application Service Poller
52
SNMP and/or network service data received
54
SNMP and/or network service data stored on Data Warehouse Server
55
network service data interpreted
56
network service data received triggers alarm
57
alarm sent to client via E-mail or pager
58
client login authentication
59
SNMP data graphed and sent to end-user workstation
60
client terminates session
61

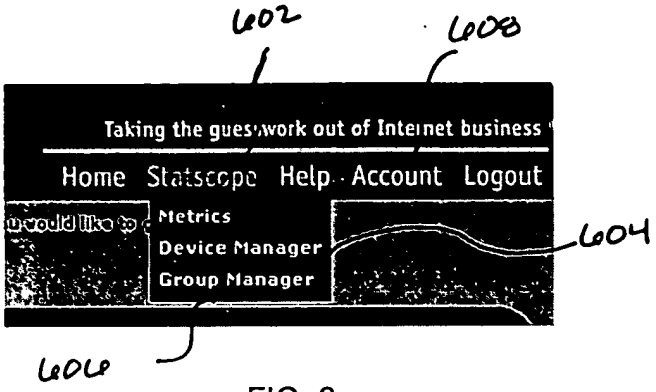


FIG. 6

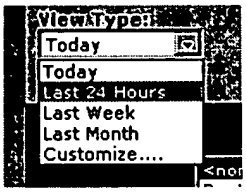


FIG. 7

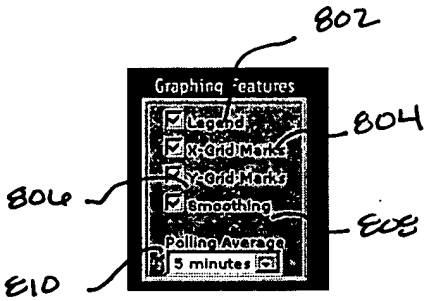


FIG. 8

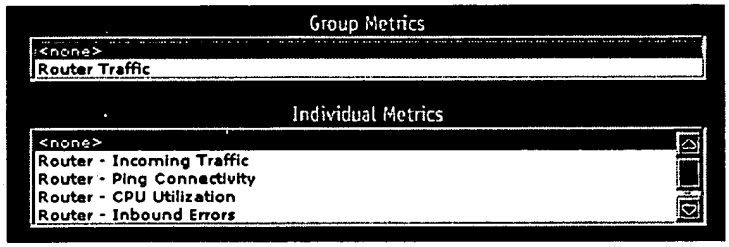


FIG. 9

Edit Monitor

Functionality

Polling: ☑

Notifications: ☐

Primary Contact

Primary Email:

Primary Pager:

Secondary Contact

Email:

Pager:

Tertiary Contact

Email:

Pager:

Escalation Delay

Primary Level: 0

Secondary Level: 0

Tertiary Level: 0

Thresholds:

High: -1

Low: -1

Update Monitor

FIG. 10

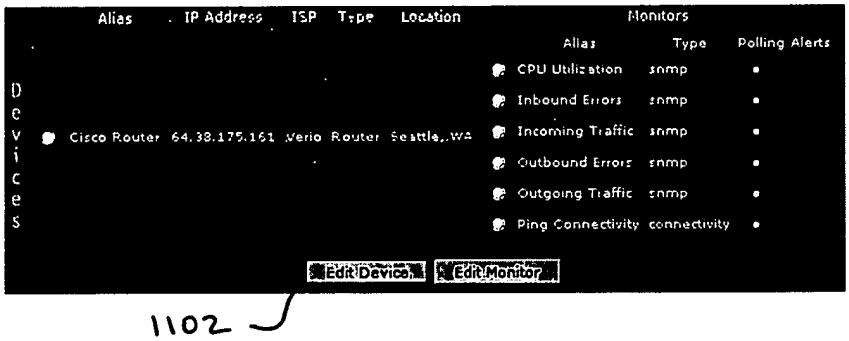


FIG. 11

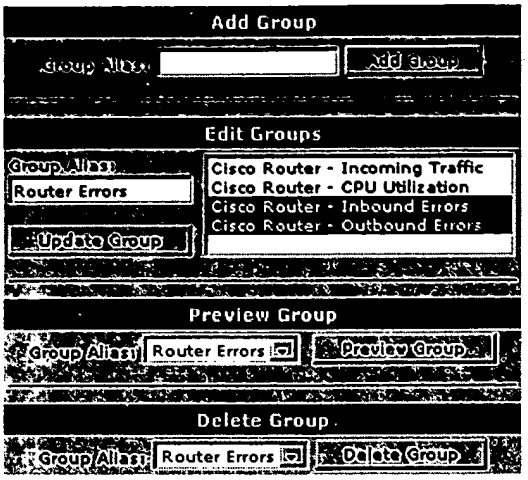

Add Group
Group Alias:
Add Group
Edit Groups
Group Alias:
Router Errors
Update Group
Cisco Router - Incoming Traffic
Cisco Router - CPU Utilization
Cisco Router - Inbound Errors
Cisco Router - Outbound Errors
Preview Group
Group Alias:
Router Errors
Preview Group
Delete Group
Group Alias:
Router Errors
Delete Group

FIG. 12

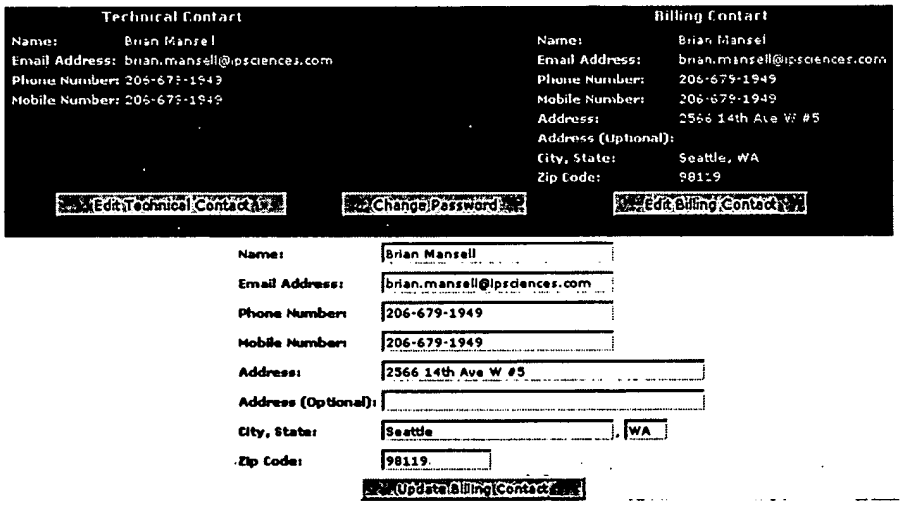

Technical Contact
Name: Brian Mansel
Email Address: brian.mansell@ipsciences.com
Phone Number: 206-679-1949
Mobile Number: 206-679-1949
Billing Contact
Name: Brian Mansel
Email Address: brian.mansell@ipsciences.com
Phone Number: 206-679-1949
Mobile Number: 206-679-1949
Address: 2566 14th Ave W #5
Address (Optional):
City, State: Seattle, WA
Zip Code: 98119
Edit Technical Contact
Change Password
Edit Billing Contact
Name: Brian Mansell
Email Address: brian.mansell@ipsciences.com
Phone Number: 206-679-1949
Mobile Number: 206-679-1949
Address: 2566 14th Ave W #5
Address (Optional):
City, State: Seattle, WA
Zip Code: 98119
Update Billing Contact

FIG. 13

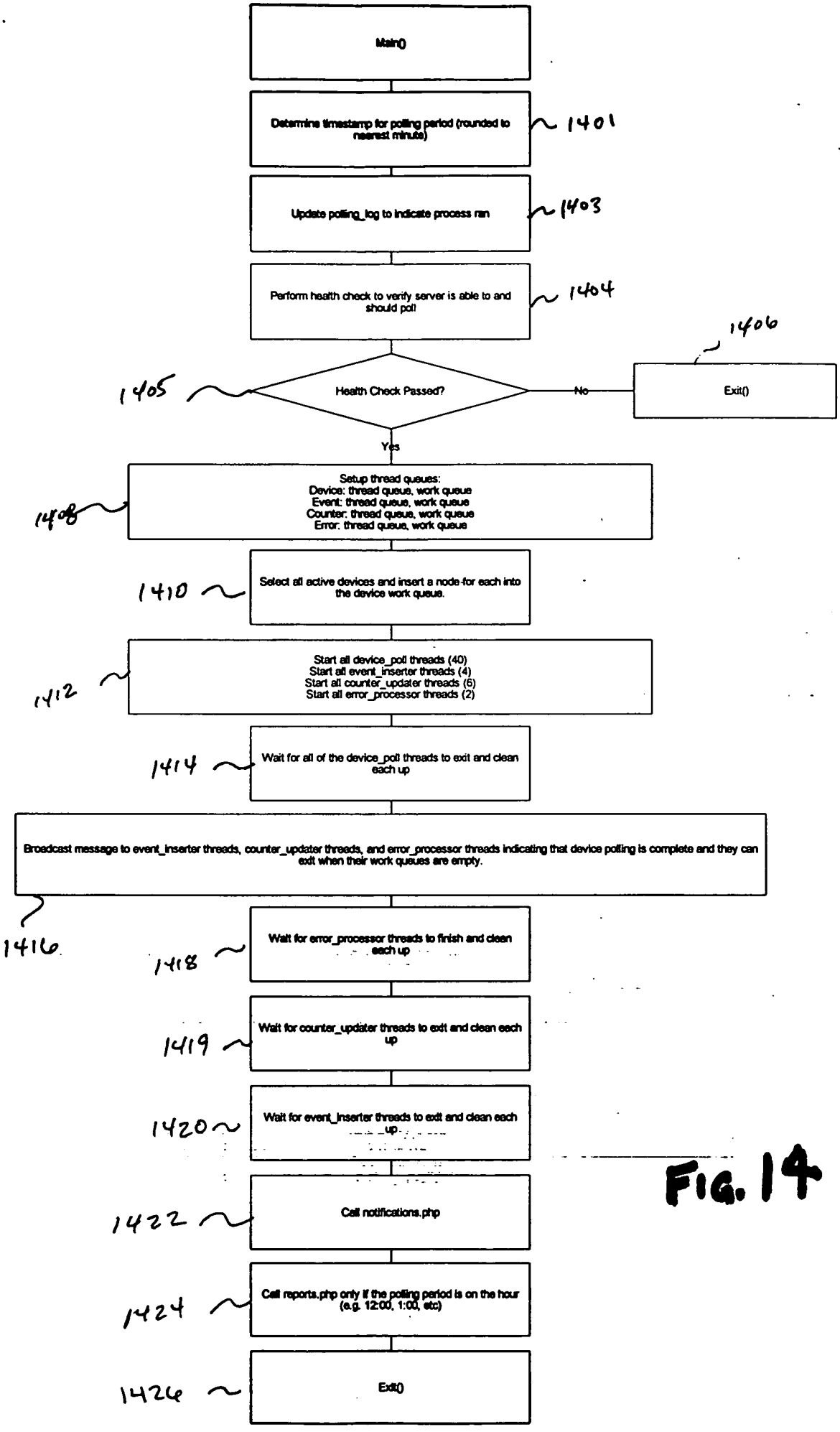
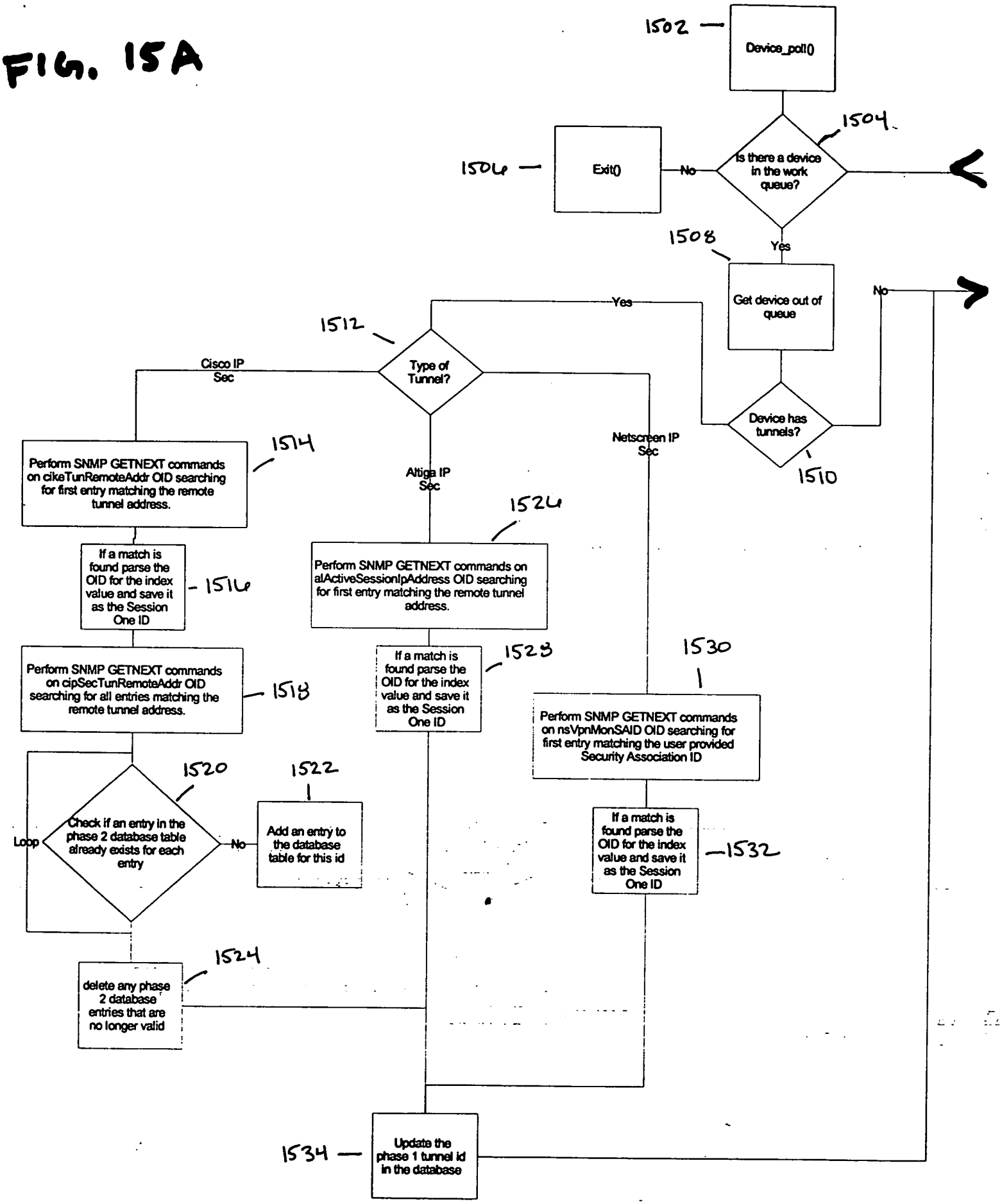

Main()
Determine timestamp for polling period (rounded to nearest minute)
1401
Update polling_log to indicate process ran
1403
Perform health check to verify server is able to and should poll
1404
1406
1405
Health Check Passed?
No
Exit()
Yes
1408
Setup thread queues:
Device: thread queue, work queue
Event: thread queue, work queue
Counter: thread queue, work queue
Error: thread queue, work queue
1410
Select all active devices and insert a node for each into the device work queue.
1412
Start all device_poll threads (40)
Start all event_inserter threads (4)
Start all counter_updater threads (6)
Start all error_processor threads (2)
1414
Wait for all of the device_poll threads to exit and clean each up
Broadcast message to event_inserter threads, counter_updater threads, and error_processor threads indicating that device polling is complete and they can exit when their work queues are empty.
1416
1418
Wait for error_processor threads to finish and clean each up
1419
Wait for counter_updater threads to exit and clean each up
1420
Wait for event_inserter threads to exit and clean each up
1422
Call notifications.php
1424
Call reports.php only if the polling period is on the hour (e.g. 12:00, 1:00, etc)
1426
Exit()

FIG. 14

FIG. 15A


1502
Device_poll()
1504
Is there a device in the work queue?
No
1506
Exit()
Yes
1508
Get device out of queue
No
Yes
1512
Type of Tunnel?
Cisco IP Sec
Altiga IP Sec
Netscreen IP Sec
Device has tunnels?
1510
1514
Perform SNMP GETNEXT commands on cikeTunRemoteAddr OID searching for first entry matching the remote tunnel address.
1516
If a match is found parse the OID for the index value and save it as the Session One ID
1518
Perform SNMP GETNEXT commands on cipSecTunRemoteAddr OID searching for all entries matching the remote tunnel address.
1520
Check if an entry in the phase 2 database table already exists for each entry
Loop
No
1522
Add an entry to the database table for this id
1524
delete any phase 2 database entries that are no longer valid
1526
Perform SNMP GETNEXT commands on alActiveSessionIpAddress OID searching for first entry matching the remote tunnel address.
1528
If a match is found parse the OID for the index value and save it as the Session One ID
1530
Perform SNMP GETNEXT commands on nsVpnMonSAID OID searching for first entry matching the user provided Security Association ID
1532
If a match is found parse the OID for the index value and save it as the Session One ID
1534
Update the phase 1 tunnel id in the database

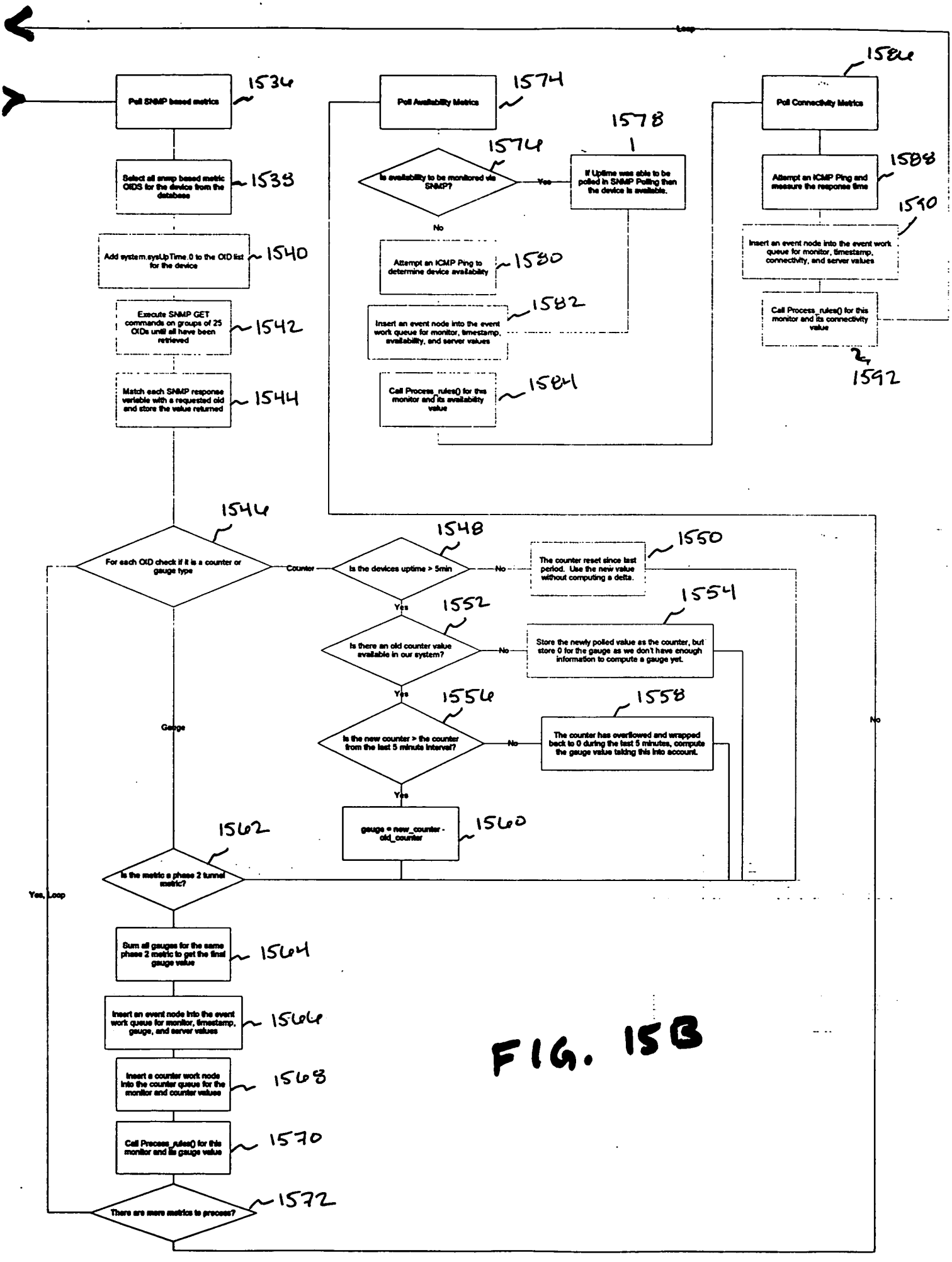

Loop
Poll SNMP based metrics
1536
Select all snmp based metric OIDS for the device from the database
1538
Add system.sysUpTime.0 to the OID list for the device
1540
Execute SNMP GET commands on groups of 25 OIDs until all have been retrieved
1542
Match each SNMP response variable with a requested oid and store the value returned
1544
Poll Availability Metrics
1574
Is availability to be monitored via SNMP?
1576
Yes
If Uptime was able to be polled in SNMP Polling then the device is available.
1578
No
Attempt an ICMP Ping to determine device availability
1580
Insert an event node into the event work queue for monitor, timestamp, availability, and server values
1582
Call Process_rules() for this monitor and its availability value
1584
Poll Connectivity Metrics
1586
Attempt an ICMP Ping and measure the response time
1588
Insert an event node into the event work queue for monitor, timestamp, connectivity, and server values
1590
Call Process_rules() for this monitor and its connectivity value
1592
For each OID check if it is a counter or gauge type
1546
Counter
Is the devices uptime > 5min
1548
No
The counter reset since last period. Use the new value without computing a delta.
1550
Yes
Is there an old counter value available in our system?
1552
No
Store the newly polled value as the counter, but store 0 for the gauge as we don't have enough information to compute a gauge yet.
1554
Yes
Is the new counter > the counter from the last 5 minute interval?
1556
No
The counter has overflowed and wrapped back to 0 during the last 5 minutes, compute the gauge value taking this into account.
1558
Yes
gauge = new_counter - old_counter
1560
Gauge
No
Is the metric a phase 2 tunnel metric?
1562
Yes, Loop
Sum all gauges for the same phase 2 metric to get the final gauge value
1564
Insert an event node into the event work queue for monitor, timestamp, gauge, and server values
1566
Insert a counter work node into the counter queue for the monitor and counter values
1568
Call Process_rules() for this monitor and its gauge value
1570
There are more metrics to process?
1572

FIG. 15B

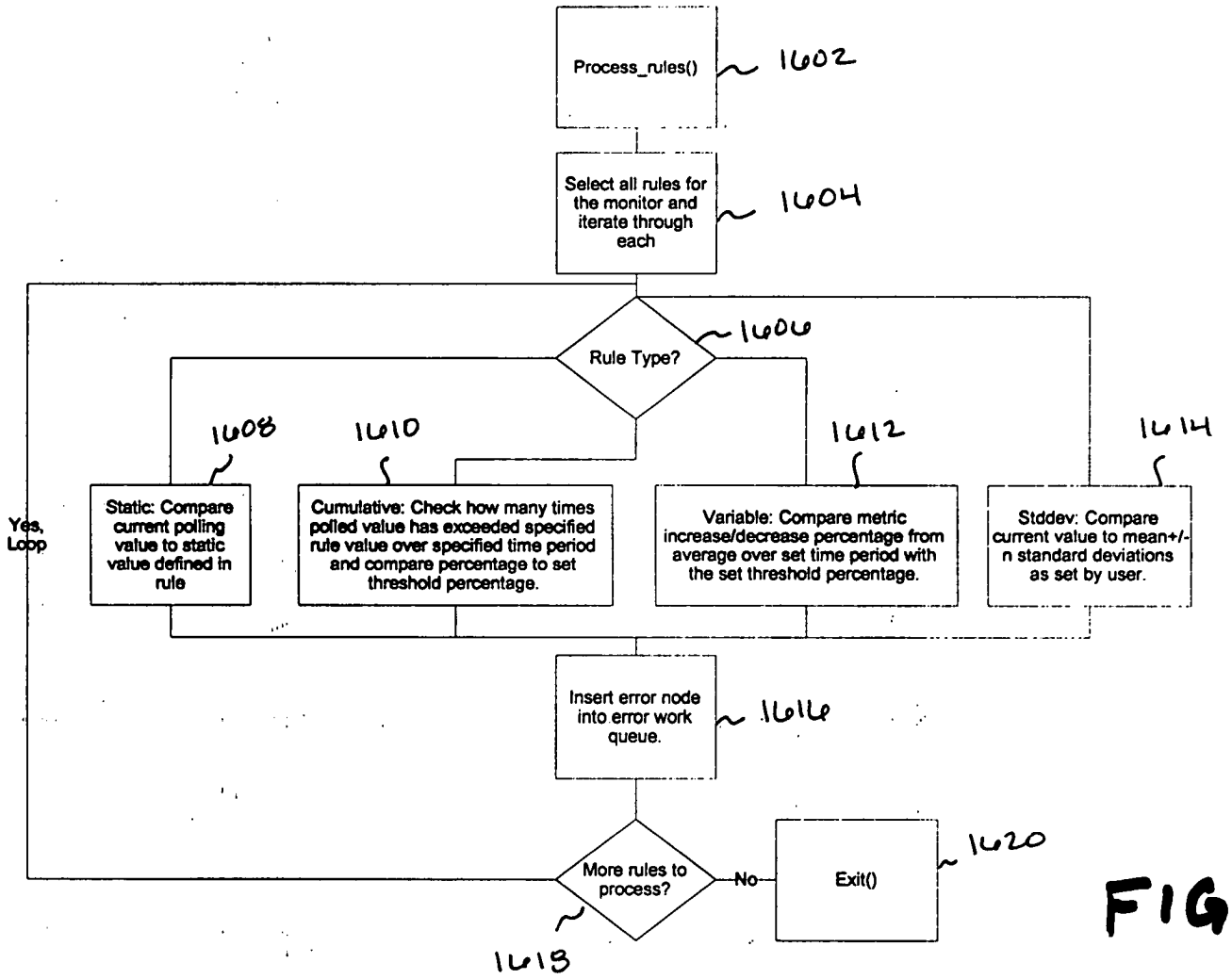

Process_rules()
1602
Select all rules for the monitor and iterate through each
1604
Rule Type?
1606
1608
1610
1612
1614
Static: Compare current polling value to static value defined in rule
Cumulative: Check how many times polled value has exceeded specified rule value over specified time period and compare percentage to set threshold percentage.
Variable: Compare metric increase/decrease percentage from average over set time period with the set threshold percentage.
Stddev: Compare current value to mean+/- n standard deviations as set by user.
Yes, Loop
Insert error node into error work queue.
1616
More rules to process?
1618
No
Exit()
1620

FIG. 16

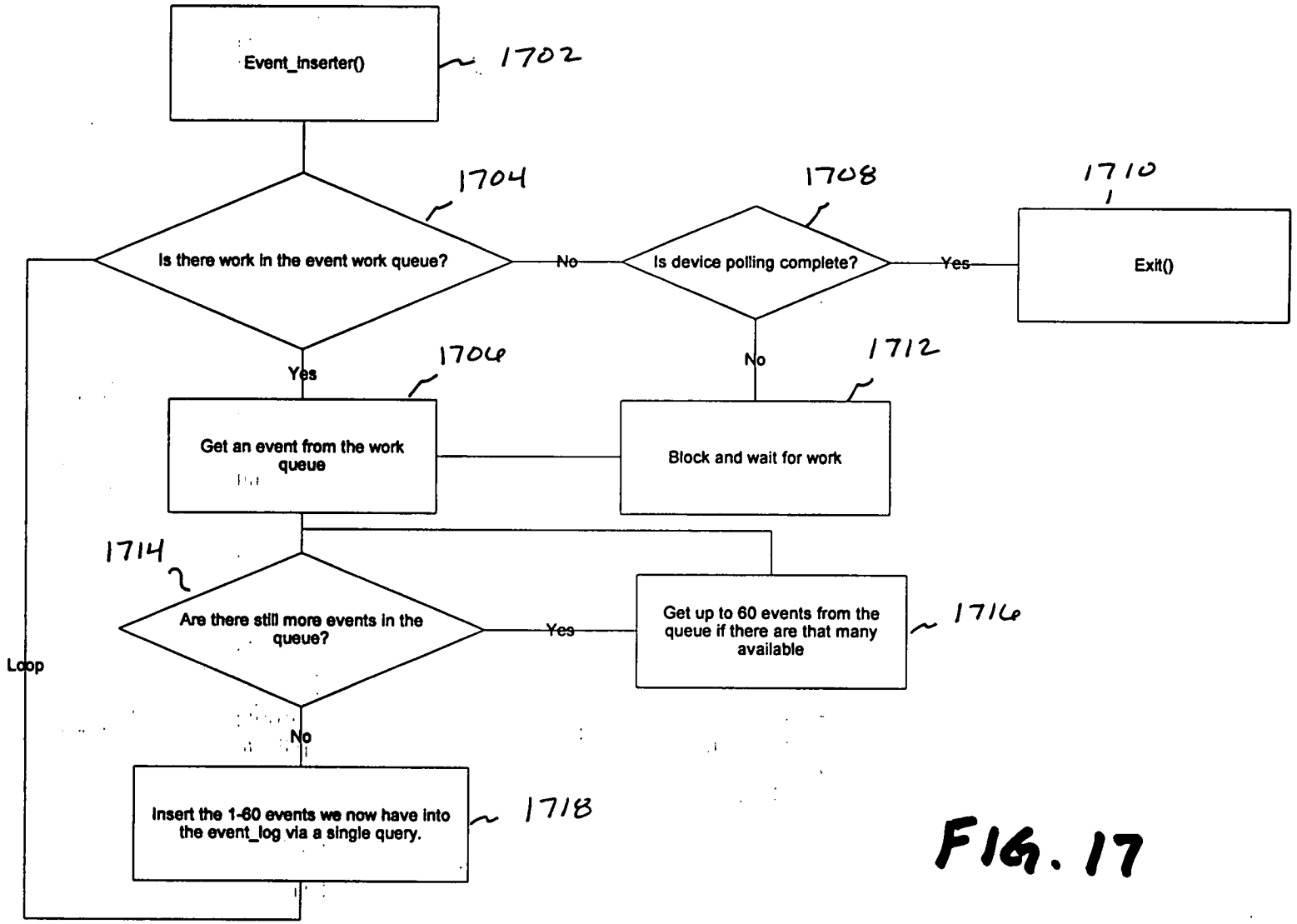

Event_inserter()
1702
Is there work in the event work queue?
1704
No
Is device polling complete?
1708
Yes
Exit()
1710
Yes
No
1706
Get an event from the work queue
Block and wait for work
1712
1714
Are there still more events in the queue?
Yes
Get up to 60 events from the queue if there are that many available
1716
Loop
No
Insert the 1-60 events we now have into the event_log via a single query.
1718

FIG. 17

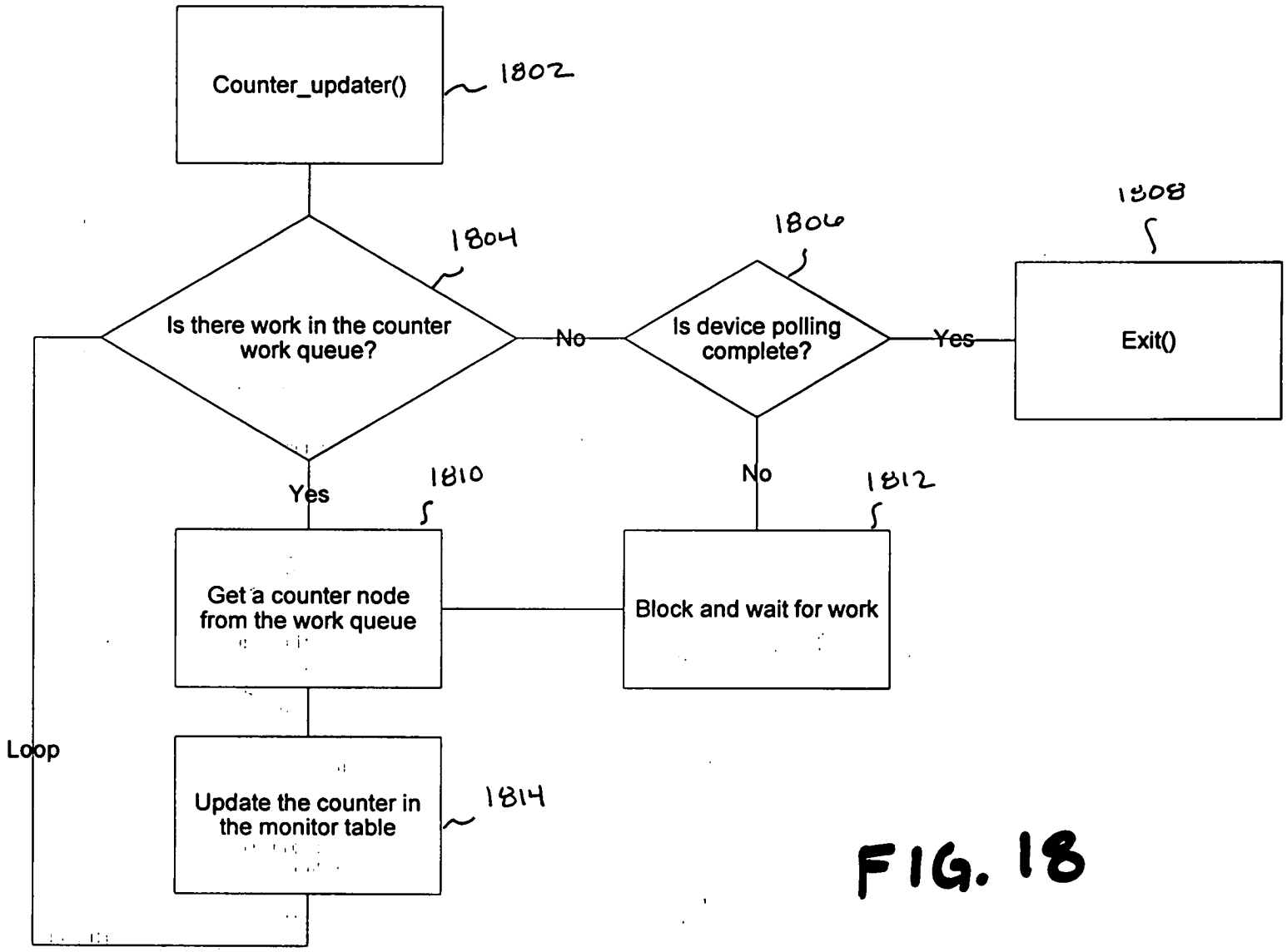
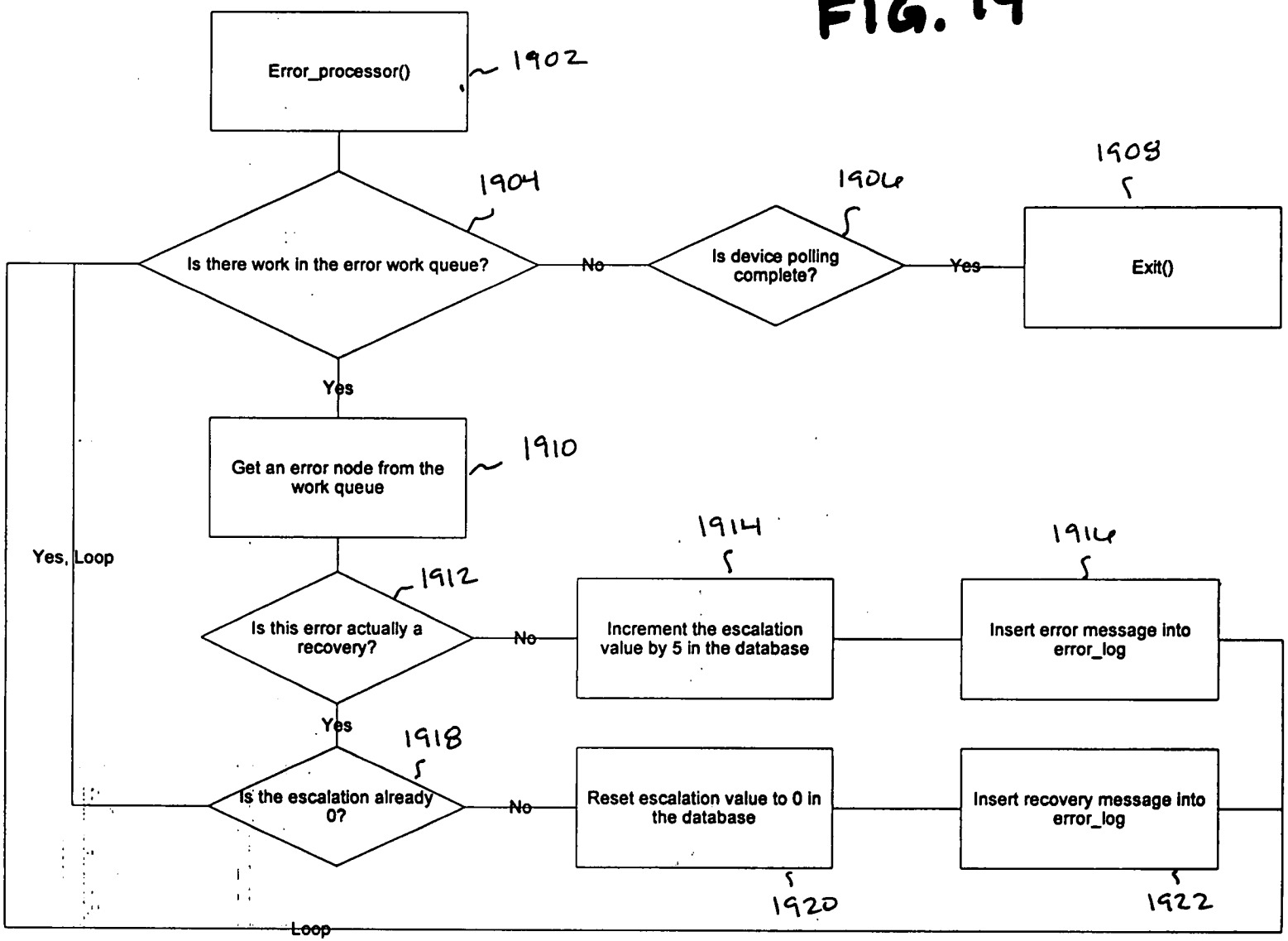

Counter_updater()
1802
Is there work in the counter work queue?
1804
No
Is device polling complete?
1806
Yes
Exit()
1808
Yes
1810
No
1812
Get a counter node from the work queue
Block and wait for work
Loop
Update the counter in the monitor table
1814

FIG. 18

FIG. 19


Error_processor()
1902
Is there work in the error work queue?
1904
No
Is device polling complete?
1906
Yes
Exit()
1908
Yes
Get an error node from the work queue
1910
Yes, Loop
Is this error actually a recovery?
1912
No
Increment the escalation value by 5 in the database
1914
Insert error message into error_log
1916
Yes
Is the escalation already 0?
1918
No
Reset escalation value to 0 in the database
1920
Insert recovery message into error_log
1922
Loop

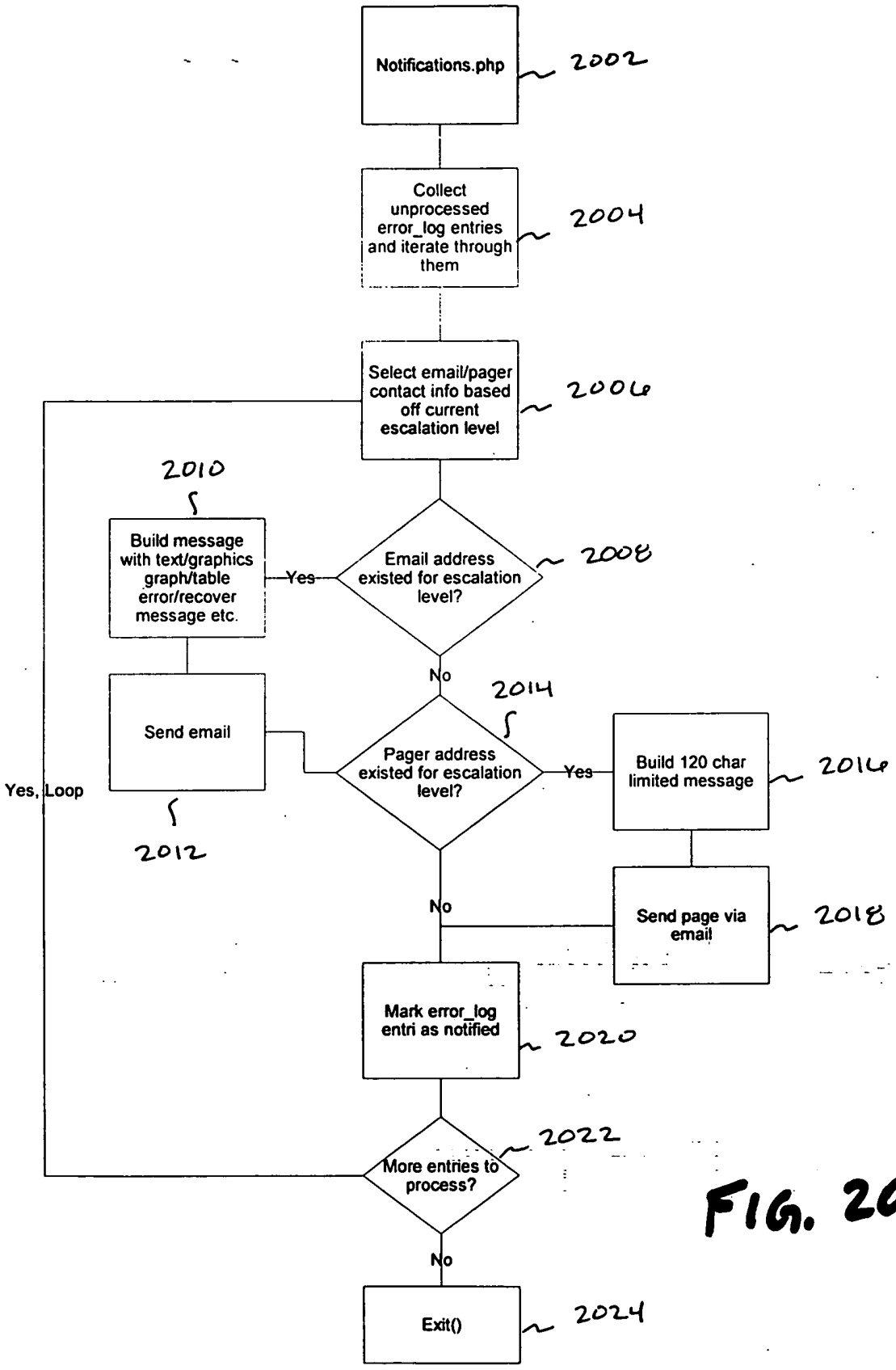

Notifications.php
2002
Collect unprocessed error_log entries and iterate through them
2004
Select email/pager contact info based off current escalation level
2006
2010
Build message with text/graphics graph/table error/recover message etc.
Yes
Email address existed for escalation level?
2008
No
2014
Send email
Pager address existed for escalation level?
Yes
Build 120 char limited message
2016
Yes, Loop
2012
No
Send page via email
2018
Mark error_log entri as notified
2020
More entries to process?
2022
No
Exit()
2024

FIG. 20

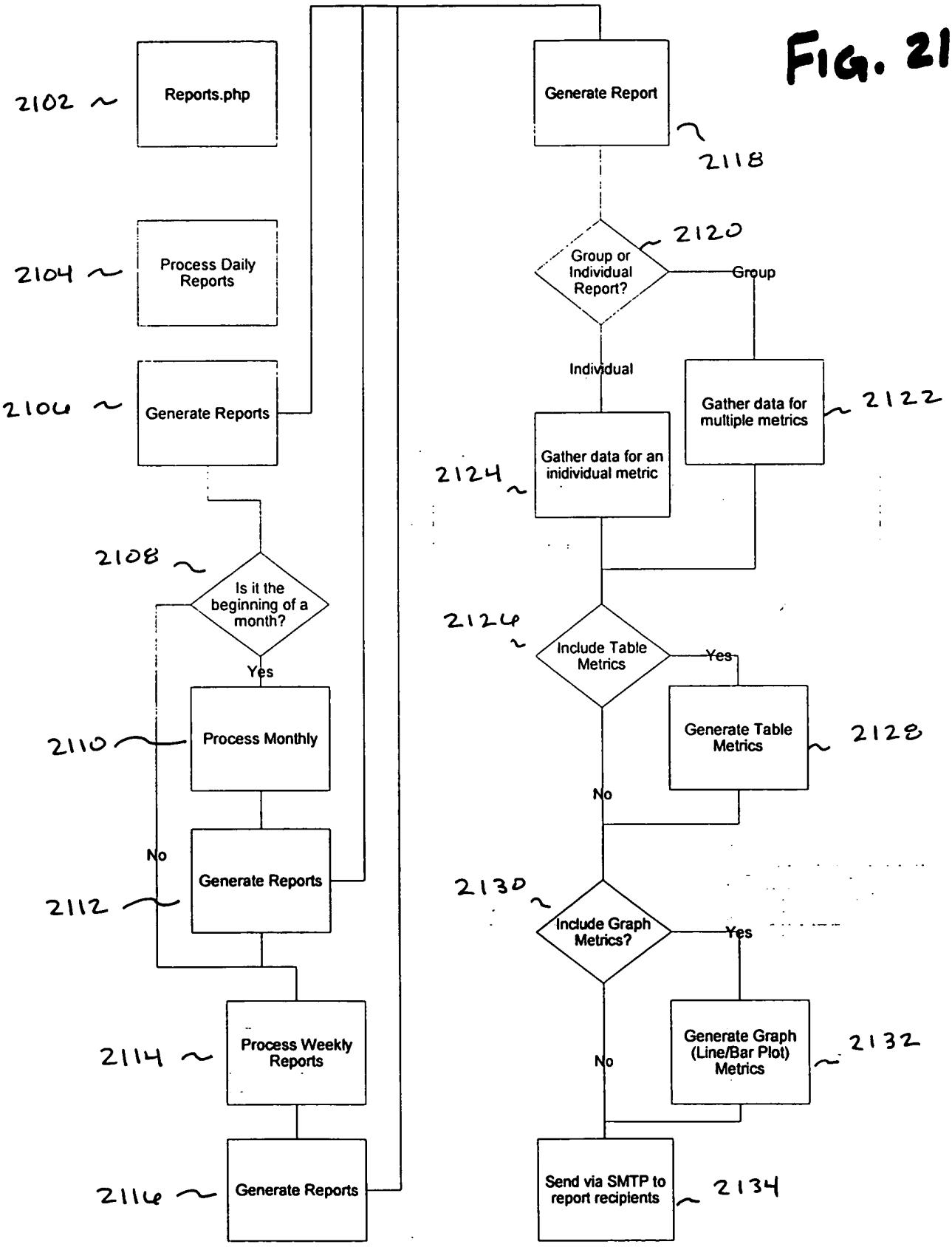

2102
Reports.php
2104
Process Daily Reports
2106
Generate Reports
2108
Is it the beginning of a month?
Yes
2110
Process Monthly
No
2112
Generate Reports
2114
Process Weekly Reports
2116
Generate Reports
Generate Report
2118
2120
Group or Individual Report?
Group
Individual
Gather data for multiple metrics
2122
Gather data for an inidividual metric
2124
2126
Include Table Metrics
Yes
Generate Table Metrics
2128
No
2130
Include Graph Metrics?
Yes
Generate Graph (Line/Bar Plot) Metrics
2132
No
Send via SMTP to report recipients
2134

FIG. 21

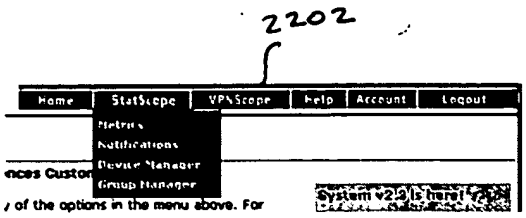


FIG. 22

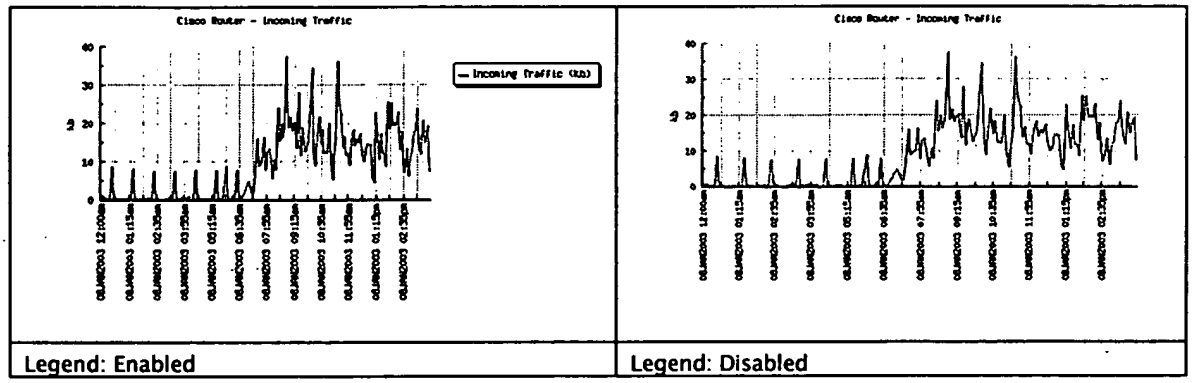


FIG. 23

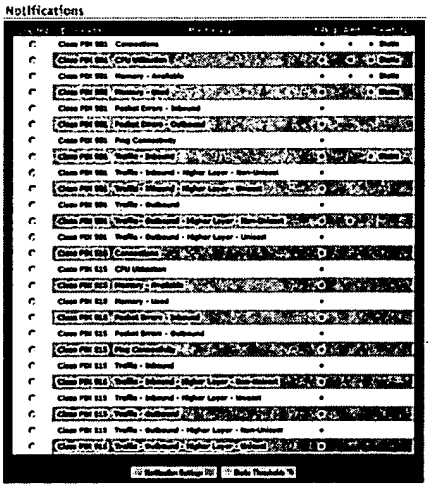


FIG. 24

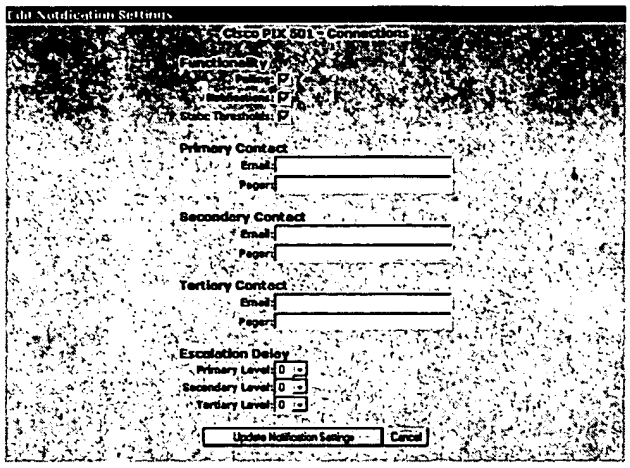


FIG. 25

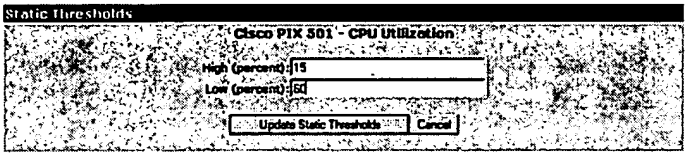


FIG. 26

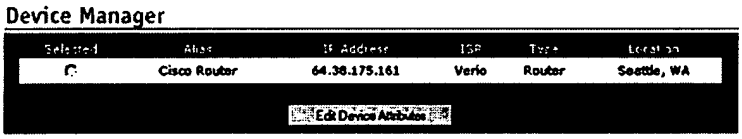


FIG. 27

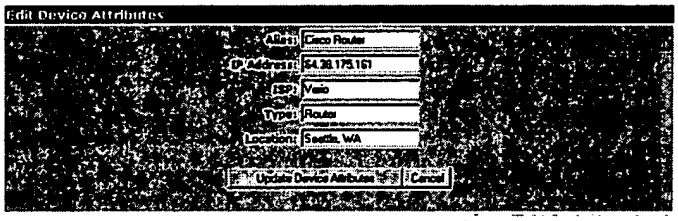


FIG. 28

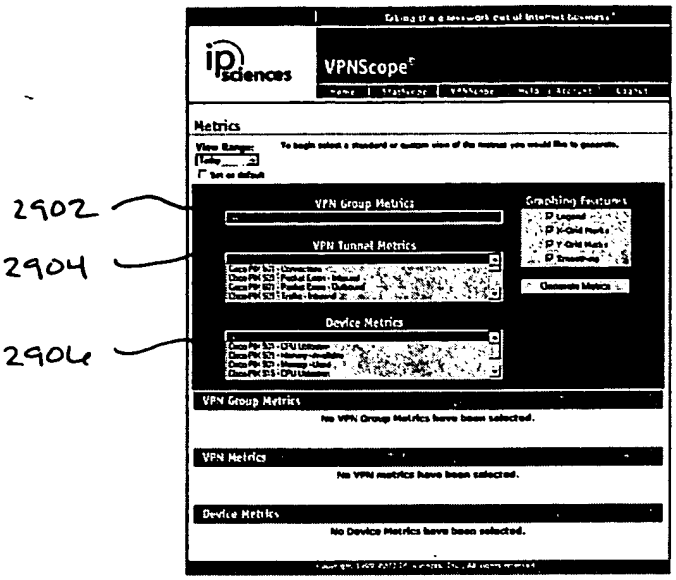


FIG. 29

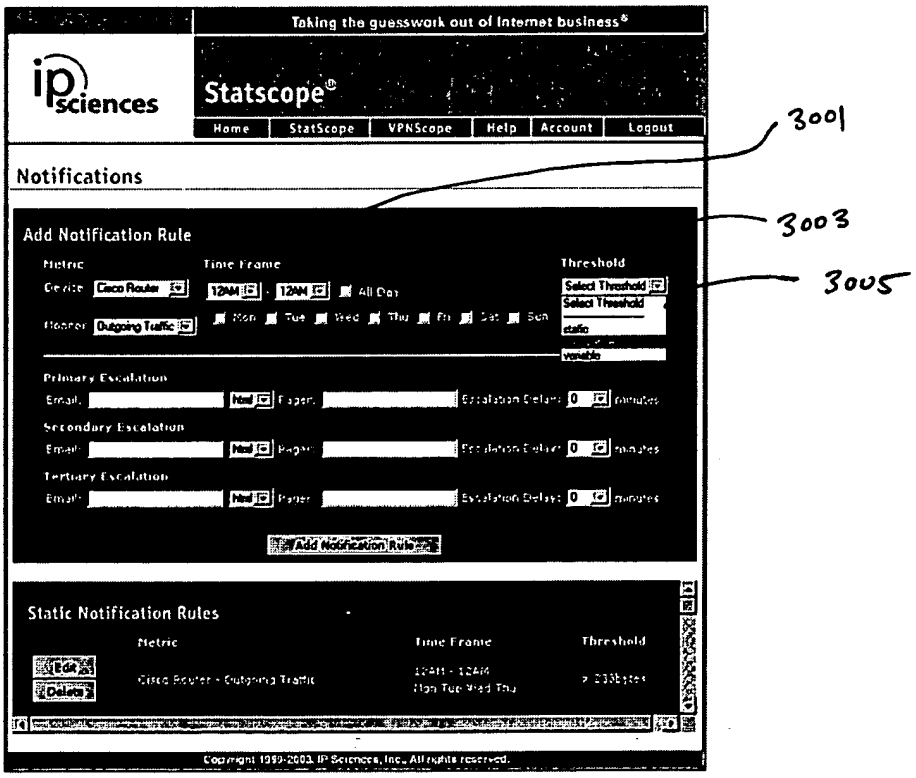


FIG. 30A

Alert Rules

	Day(s)	Time	Threshold Type	Threshold	Metric(s)
◉	All Week	All Day	Cumulative	exceeds 45.00 percent for 40% of polling periods over 15 hours	Orange Router - CPU Utilization
○	All Week	All Day	Static	exceeds 45.00 percent	Cisco Router - CPU Utilization
○	All Week	All Day	Variable	increases by a unit value of 13.67 kbps over 14 hours	dev01 - eth3 - Inbound Traffic dev01 - interface - Inbound Traffic
○	All Week	All Day	Variable	increases by a percentage value of 45% over 11 hours	Cisco Router - External - Inbound Traffic dev01 - interface - Inbound Traffic

FIG. 30B

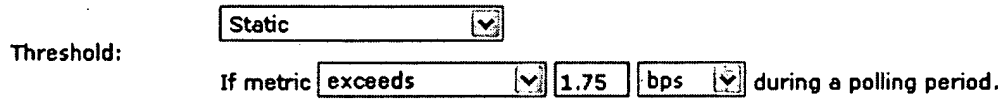


FIG. 31A

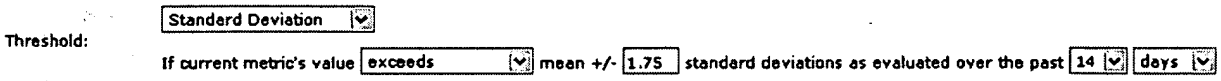


FIG. 31B

FIG. 32A

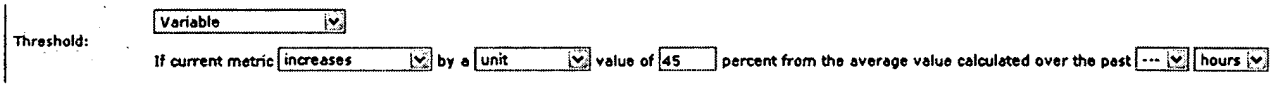


FIG. 32B

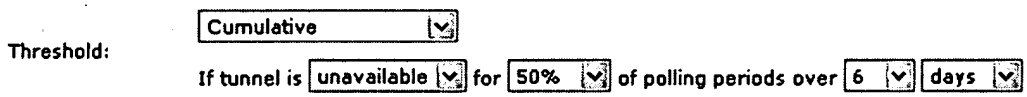


FIG. 33

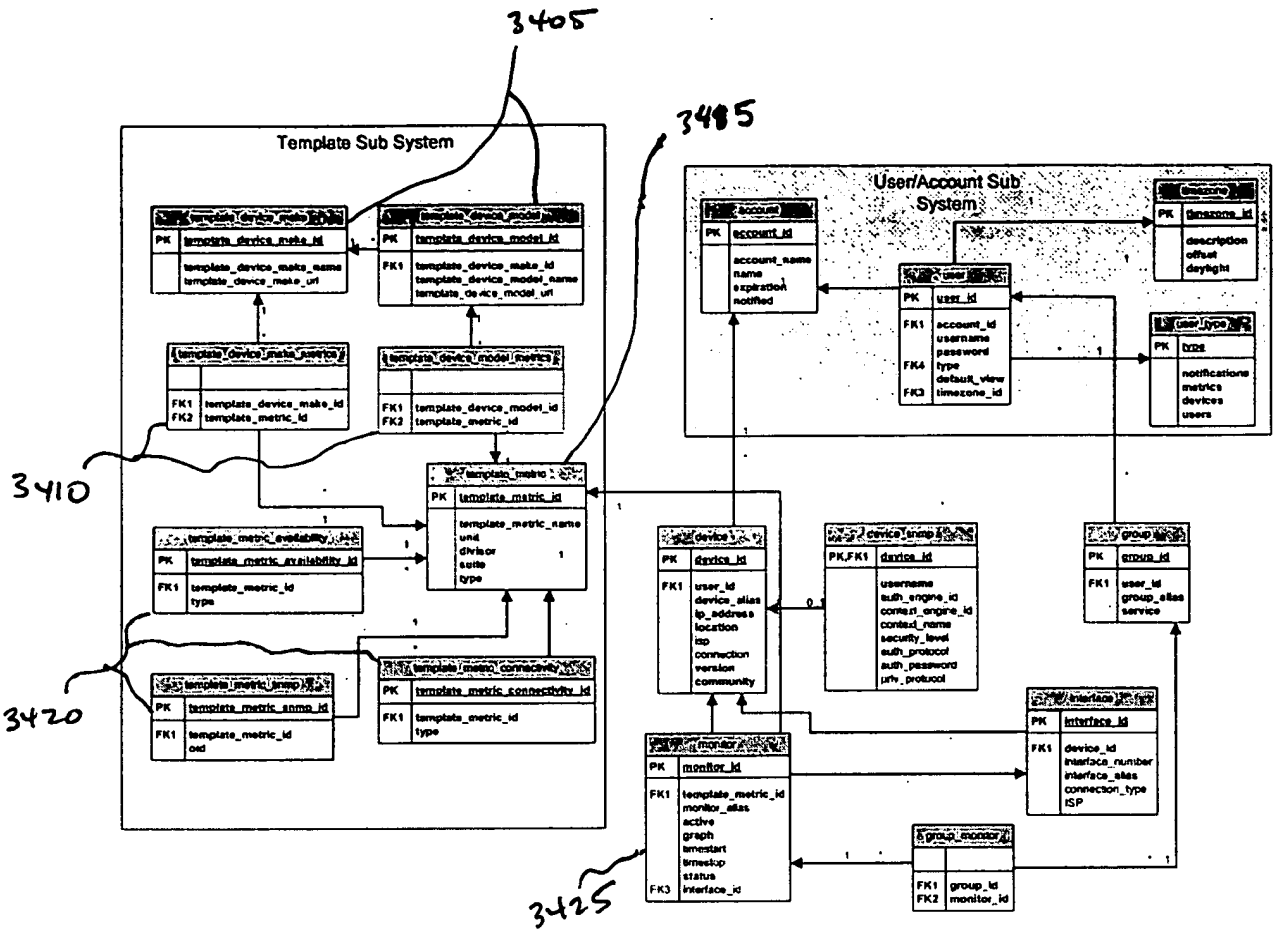

3405
3485
Template Sub System
User/Account Sub System
3410
3420
3425

FIG. 34

FIG. 35

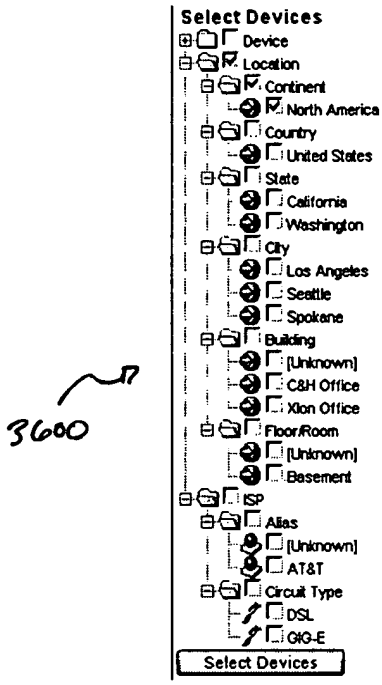

Select Devices
Device
Location
Continent
North America
Country
United States
State
California
Washington
City
Los Angeles
Seattle
Spokane
Building
[Unknown]
C&H Office
Xion Office
Floor/Room
[Unknown]
Basement
ISP
Alias
[Unknown]
AT&T
Circuit Type
DSL
GIG-E
Select Devices
3600

FIG. 36

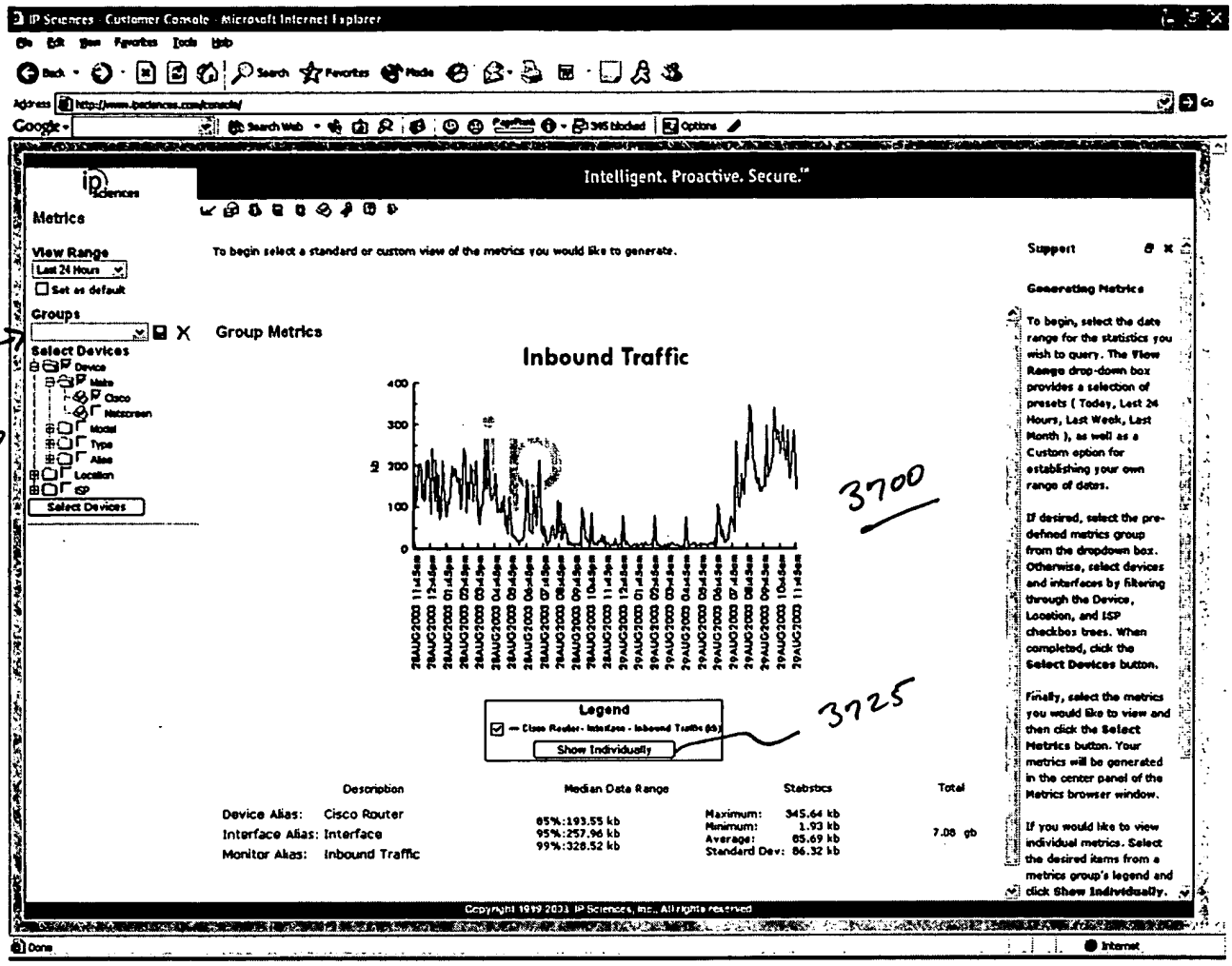

IP Sciences - Customer Console - Microsoft Internet Explorer
Intelligent. Proactive. Secure.™
Metrics
View Range
Last 24 Hours
Set as default
Groups
Select Devices
Device
Make
Cisco
Netscreen
Model
Type
Alias
Location
ISP
Select Devices
Group Metrics
Inbound Traffic
3710
3600
3700
3725
Legend
Show Individually
Description
Median Data Range
Statistics
Total
Device Alias: Cisco Router
Interface Alias: Interface
Monitor Alias: Inbound Traffic
85%:193.55 kb
95%:257.96 kb
99%:328.52 kb
Maximum: 345.64 kb
Minimum: 1.93 kb
Average: 85.69 kb
Standard Dev: 86.32 kb
7.08 gb
Support
Generating Metrics
To begin, select the date range for the statistics you wish to query. The View Range drop-down box provides a selection of presets (Today, Last 24 Hours, Last Week, Last Month), as well as a Custom option for establishing your own range of dates.
If desired, select the pre-defined metrics group from the dropdown box. Otherwise, select devices and interfaces by filtering through the Device, Location, and ISP checkbox trees. When completed, click the Select Devices button.
Finally, select the metrics you would like to view and then click the Select Metrics button. Your metrics will be generated in the center panel of the Metrics browser window.
If you would like to view individual metrics. Select the desired items from a metrics group's legend and click Show Individually.
Copyright 1999-2003 IP Sciences, Inc. All rights reserved
Done
Internet

FIG. 37

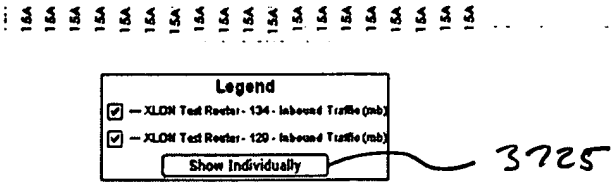

Legend
— XLON Test Router - 134 - Inbound Traffic (mb)
— XLON Test Router - 129 - Inbound Traffic (mb)
Show Individually
3725

FIG. 38

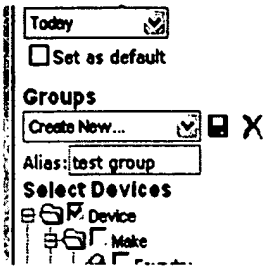

Today
Set as default
Groups
Create New...
Alias: test group
Select Devices
Device
Make

FIG. 39

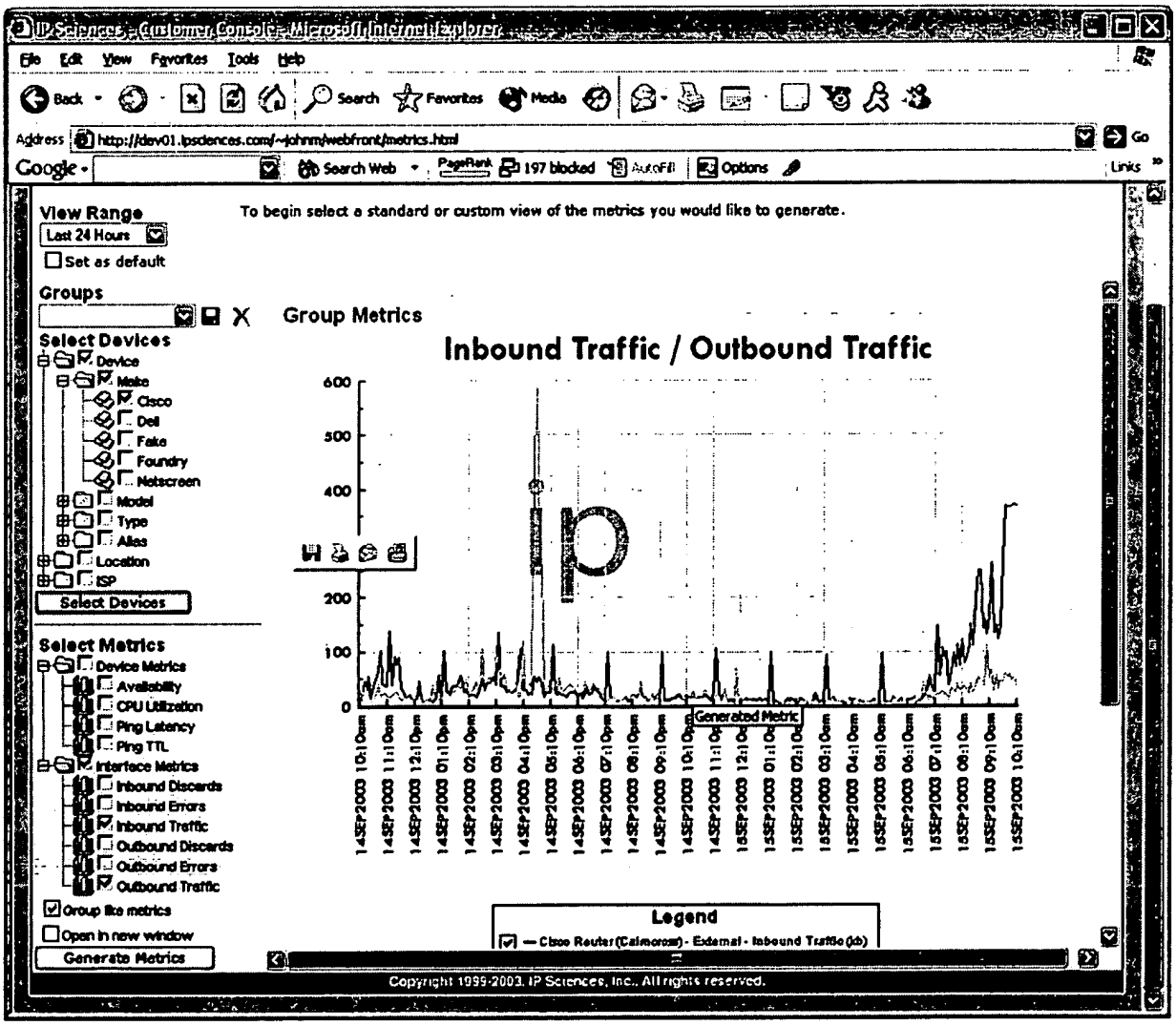

IP Sciences - Customer Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dev01.ipsciences.com/~johnm/webfront/metrics.html
Google Search Web PageRank 197 blocked AutoFill Options
Links
View Range
Last 24 Hours
Set as default
To begin select a standard or custom view of the metrics you would like to generate.
Groups
Group Metrics
Select Devices
Device
Make
Cisco
Dell
Fake
Foundry
Netscreen
Model
Type
Alias
Location
ISP
Select Devices
Select Metrics
Device Metrics
Availability
CPU Utilization
Ping Latency
Ping TTL
Interface Metrics
Inbound Discards
Inbound Errors
Inbound Traffic
Outbound Discards
Outbound Errors
Outbound Traffic
Group like metrics
Open in new window
Generate Metrics
Inbound Traffic / Outbound Traffic
600
500
400
200
100
0
Generated Metric
Legend
Copyright 1999-2003, IP Sciences, Inc., All rights reserved.

FIG. 40

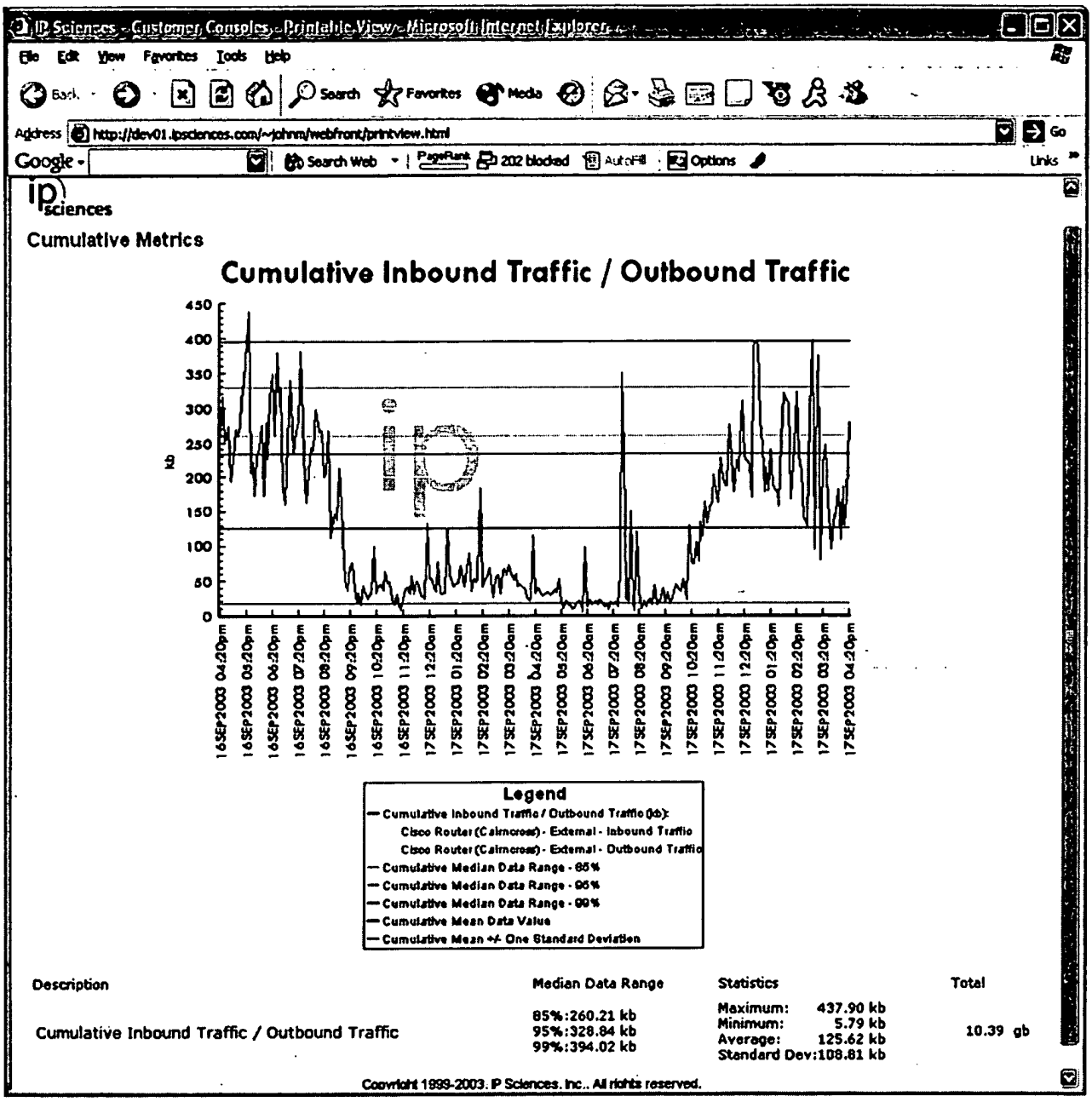

IP Sciences - Customer Complex - Printable View - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://dev01.ipsciences.com/~johnm/webfront/printview.html
Google
ip sciences
Cumulative Metrics
Cumulative Inbound Traffic / Outbound Traffic
Legend
Cumulative Inbound Traffic / Outbound Traffic (kb):
Cisco Router (Calmcrest) - External - Inbound Traffic
Cisco Router (Calmcrest) - External - Outbound Traffic
Cumulative Median Data Range - 85%
Cumulative Median Data Range - 95%
Cumulative Median Data Range - 99%
Cumulative Mean Data Value
Cumulative Mean +/- One Standard Deviation
Description
Median Data Range
Statistics
Total
Cumulative Inbound Traffic / Outbound Traffic
85%:260.21 kb
95%:328.84 kb
99%:394.02 kb
Maximum: 437.90 kb
Minimum: 5.79 kb
Average: 125.62 kb
Standard Dev: 108.81 kb
10.39 gb
Copyright 1999-2003. IP Sciences, Inc., All rights reserved.

FIG. 41

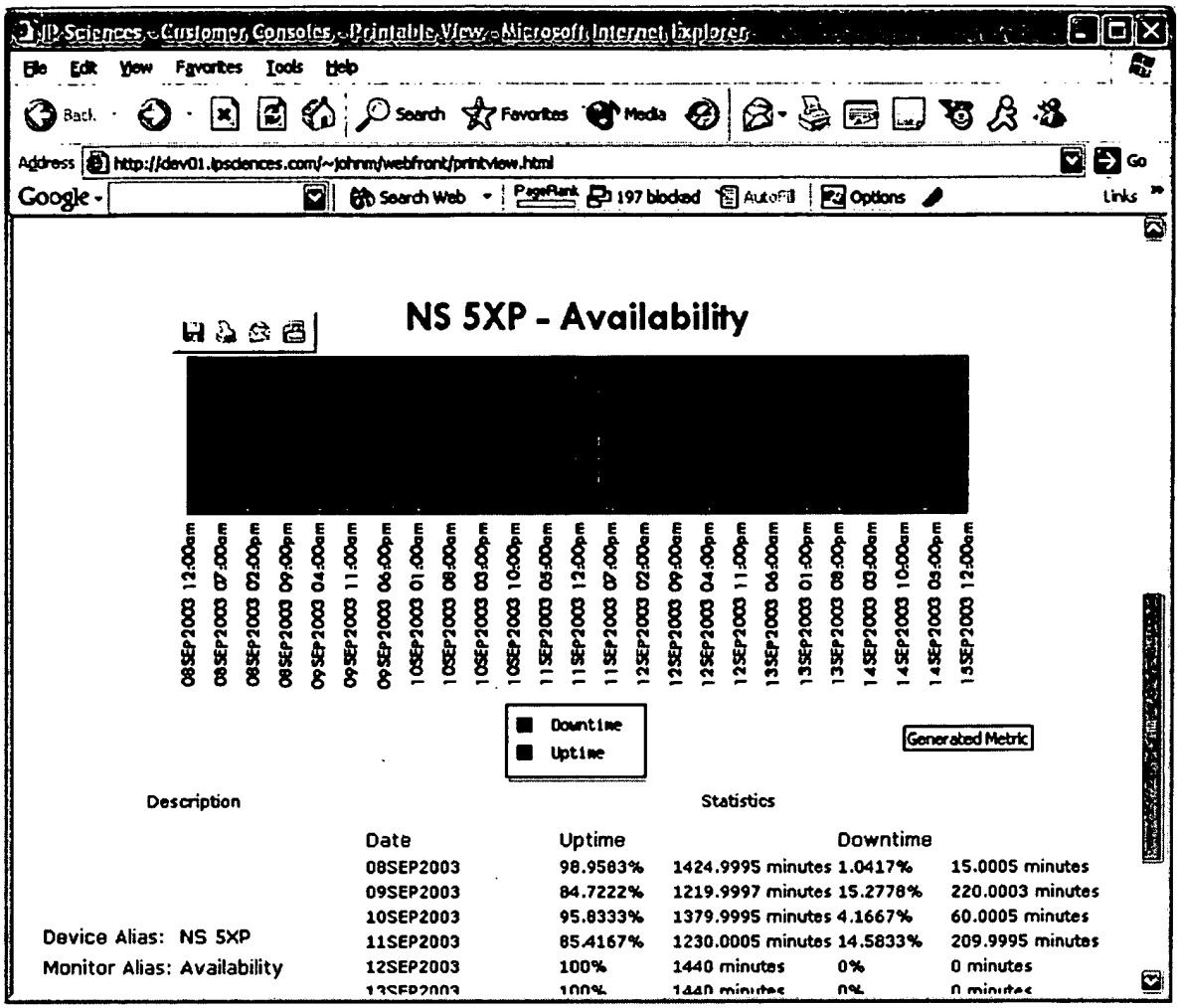

IP Sciences - Customer Consoles - Printable View - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dev01.ipsciences.com/~johnm/webfront/printview.html
Go
Google Search Web PageRank 197 blocked AutoFill Options
Links
NS 5XP - Availability
08SEP2003 12:00am
08SEP2003 07:00am
08SEP2003 02:00pm
08SEP2003 09:00pm
09SEP2003 04:00am
09SEP2003 11:00am
09SEP2003 06:00pm
10SEP2003 01:00am
10SEP2003 08:00am
10SEP2003 03:00pm
10SEP2003 10:00pm
11SEP2003 05:00am
11SEP2003 12:00pm
11SEP2003 07:00pm
12SEP2003 02:00am
12SEP2003 09:00am
12SEP2003 04:00pm
12SEP2003 11:00pm
13SEP2003 06:00am
13SEP2003 01:00pm
13SEP2003 08:00pm
14SEP2003 03:00am
14SEP2003 10:00am
14SEP2003 05:00pm
15SEP2003 12:00am
Downtime
Uptime
Generated Metric
Description
Statistics
Device Alias: NS 5XP
Monitor Alias: Availability
Date
Uptime
Downtime
08SEP2003 98.9583% 1424.9995 minutes 1.0417% 15.0005 minutes
09SEP2003 84.7222% 1219.9997 minutes 15.2778% 220.0003 minutes
10SEP2003 95.8333% 1379.9995 minutes 4.1667% 60.0005 minutes
11SEP2003 85.4167% 1230.0005 minutes 14.5833% 209.9995 minutes
12SEP2003 100% 1440 minutes 0% 0 minutes

FIG. 42

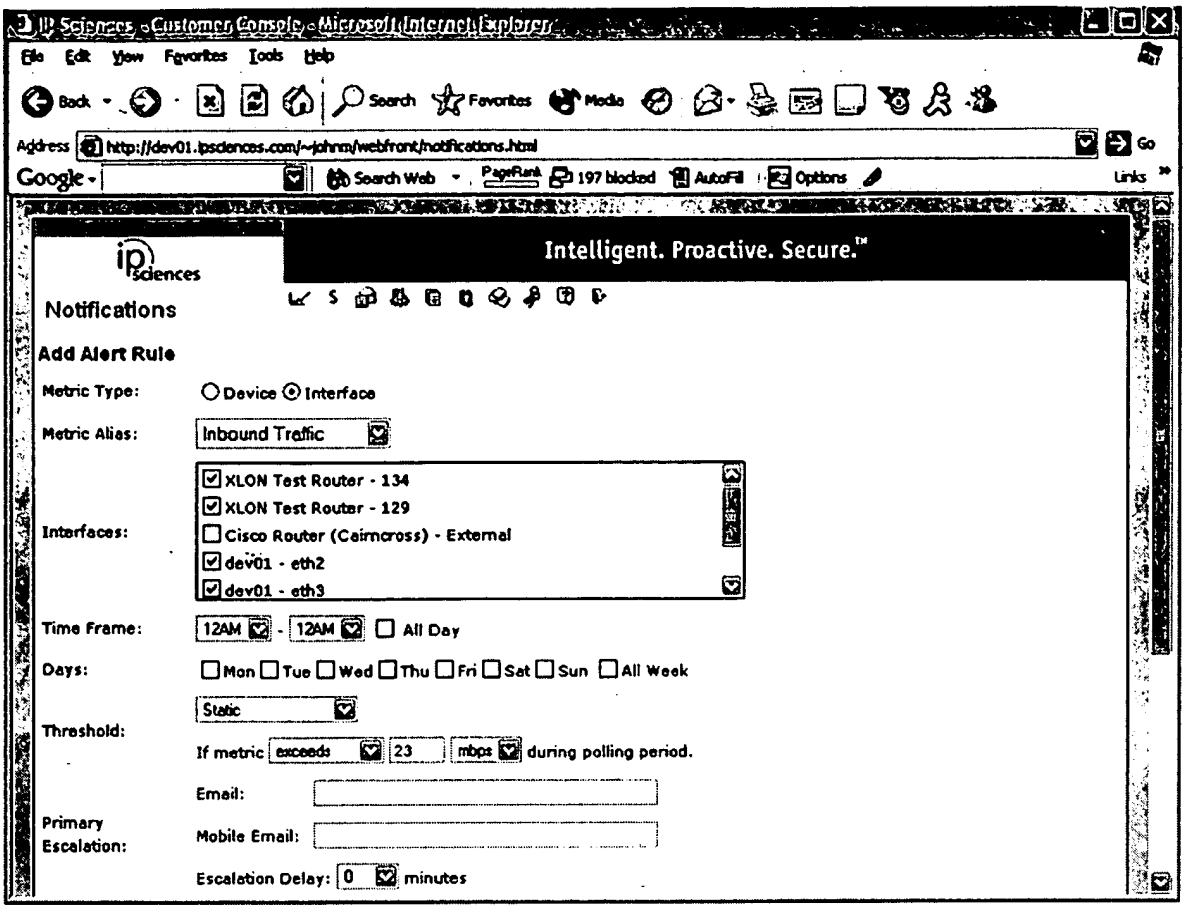

IP Sciences Customer Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dev01.ipsciences.com/~johnm/webfront/notifications.html
Go
Google Search Web PageRank 197 blocked AutoFill Options
Links
ip sciences
Intelligent. Proactive. Secure.™
Notifications
Add Alert Rule
Metric Type: Device Interface
Metric Alias: Inbound Traffic
Interfaces:
XLON Test Router - 134
XLON Test Router - 129
Cisco Router (Cairncross) - External
dev01 - eth2
dev01 - eth3
Time Frame: 12AM - 12AM All Day
Days: Mon Tue Wed Thu Fri Sat Sun All Week
Threshold: Static
If metric exceeds 23 mbps during polling period.
Primary Escalation: Email:
Mobile Email:
Escalation Delay: 0 minutes

FIG. 43

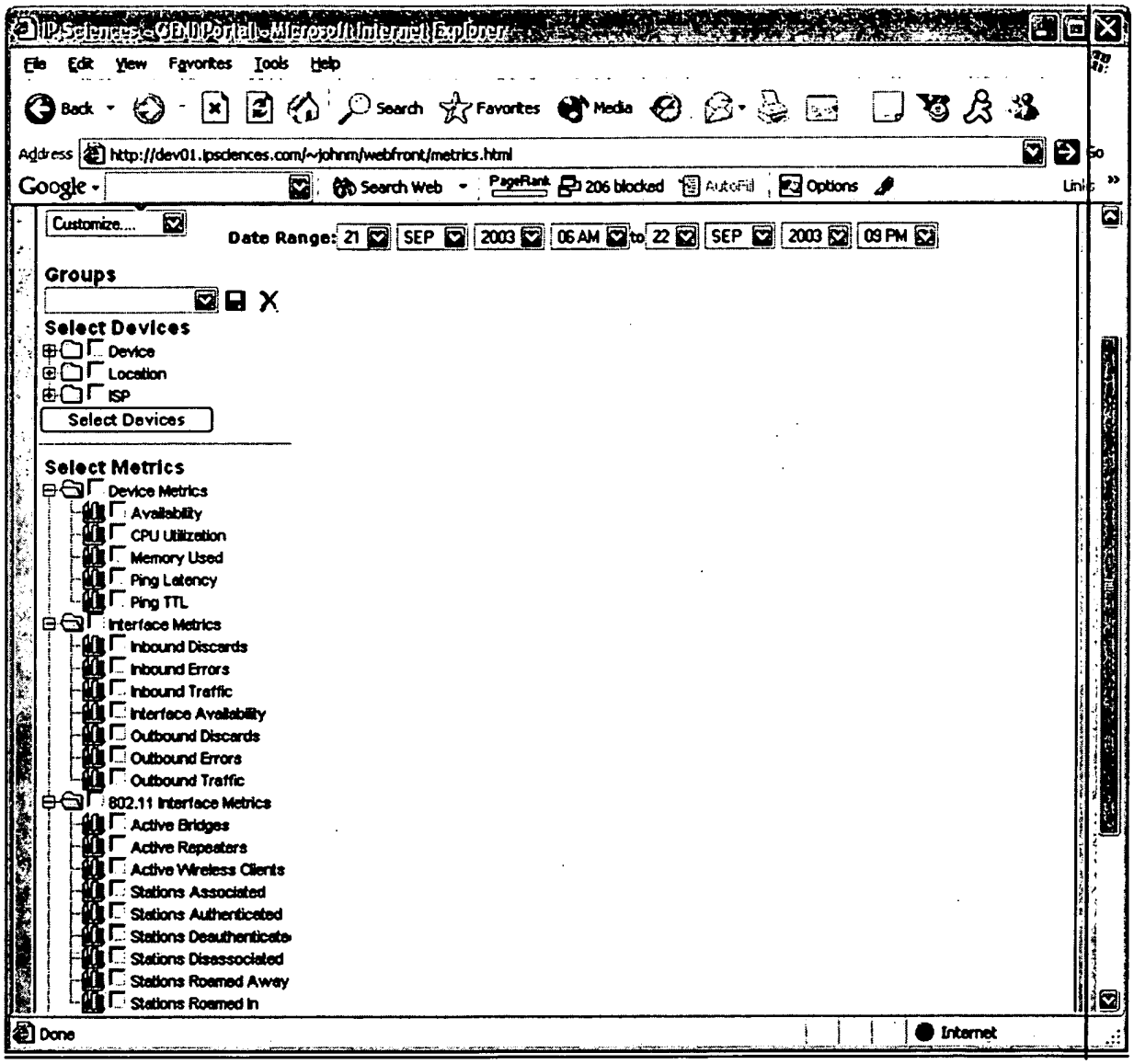

IPSciences CDN Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dev01.ipsciences.com/~johnm/webfront/metrics.html
Google Search Web PageRank 206 blocked AutoFill Options
Customize....
Date Range: 21 SEP 2003 06 AM to 22 SEP 2003 09 PM
Groups
Select Devices
Device
Location
ISP
Select Devices
Select Metrics
Device Metrics
Availability
CPU Utilization
Memory Used
Ping Latency
Ping TTL
Interface Metrics
Inbound Discards
Inbound Errors
Inbound Traffic
Interface Availability
Outbound Discards
Outbound Errors
Outbound Traffic
802.11 Interface Metrics
Active Bridges
Active Repeaters
Active Wireless Clients
Stations Associated
Stations Authenticated
Stations Deauthenticate
Stations Disassociated
Stations Roamed Away
Stations Roamed In
Done
Internet

FIG. 44